IN THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended) An apparatus for encrypting ~~64-bit~~ N-bit plain text blocks, comprising:

input ~~buffering~~ means for receiving a plain text block byte-by-byte and outputting ~~a~~ first and ~~a~~ second ~~32-bit~~ N/2-bit plain text blocks in response to a first clock;

encryption means for performing time multiplexed encryption of the first ~~and the second 32-bit~~ N/2-bit plain text ~~blocks in response to~~ block by using the first clock and time multiplexed encryption of the second N/2-bit plain text block by using a second ~~clock,~~ clock to thereby ~~generating~~ generate ~~a~~ first and ~~a~~ second ~~32-bit~~ N/2-bit cipher text blocks; and

output ~~buffering~~ means for receiving the first and the second ~~32-bit~~ N/2-bit cipher text blocks in response to the second clock and outputting ~~eight 8-bit~~ N/8 cipher text blocks, wherein N is a positive integer.

2. (Currently Amended) The apparatus as recited in ~~claim 1~~ claim 8, wherein the encryption means includes:

a cipher function unit for receiving the first and the second 32-bit plain text blocks from the input ~~buffering~~ means in response to the first clock, encrypting the first and the second 32-bit plain text blocks using a first subkey and a second ~~subkeys~~ subkey, respectively, and outputting a first encrypted 32-bit block in response to the first clock and

a second encrypted 32-bit block in response to the second clock;

a first XOR unit for performing XOR operation of the first encrypted 32-bit block and the second 32-bit plain text, thereby generating a first encrypted block;

a second XOR unit for performing XOR operation of the second encrypted 32-bit block and the first 32-bit plain text, thereby generating a second cipher block;

a left register for storing the second cipher block and outputting the second cipher block to the cipher function unit in response to the first clock; and

a right register for storing the first cipher block and outputting the first cipher block to the cipher function unit in response to the second clock.

3. (Original) The apparatus as recited in claim 2, wherein the second clock is an inverse signal of the first clock.

4. (Original) The apparatus as recited in claim 3, wherein the cipher function unit includes:

a first expansion permutation unit for performing an expansion permutation of the left 32-bit plain text block to generate a first 48-bit block;

a second expansion permutation unit for performing an expansion permutation of the right 32-bit plain text block to generate a second 48-bit block;

a third XOR unit for performing XOR operation of the first 48-bit block and the first subkey from a key scheduler, thereby generating a first XORed 48-bit block;

a fourth XOR unit for performing XOR operation of the second 48-bit block and the second subkey from the key scheduler, thereby generating a second XORed 48-bit block;

a multiplexer for selecting one of the first and the second XORed 48-bit blocks and outputting a XORed 48-bit block in accordance a control signal;

a S-Box permutation unit for receiving the XORed 48-bit block from the multiplexer and outputting 32-bit data block;

a P-Box permutation unit for permuting the 32-bit data block from the S-Box permutation unit to generate a permuted 32-bit block; and

a demultiplexer for outputting the permuted 32-bit block to one of two output ports in accordance with the control signal.

5. (Original) The apparatus as recited in claim 4, wherein the key scheduler includes:

a first scheduling means for receiving a 56-bit key block and generating the first subkey in accordance with the first clock; and

a second scheduling means for receiving the 56-bit key block and generating the second subkey in accordance with the second clock.

6. (Original) The apparatus as recited in claim 5, wherein the first key scheduling means includes:

a first permutation choice unit for permuting the 56-bit key block;

a first register for storing left 28 bits among the 56-bit key block from the first permutation choice unit in accordance with the first clock;

a second register for storing right 28 bits among the 56-bit key block from the first permutation choice unit in accordance with the first clock;

two shifters, each for shifting the 28 bits stored in the first and the second registers

by a predetermined number of bits; and

a second permutation choice unit for permuting the 28 bits stored in the first and the second registers, thereby generating the first subkey.

7. (Original) The apparatus as recited in claim 6, wherein the second key scheduling means includes:

a third permutation choice unit for permuting the 56-bit key block;

a third register for storing left 28 bits among the 56-bit key block from the third permutation choice unit in accordance with the second clock;

a fourth register for storing right 28 bits among the 56-bit key block from the third permutation choice unit in accordance with the second clock;

two shifters, each for shifting the 28 bits stored in the third and the fourth registers by a predetermined number of bits; and

a fourth permutation choice unit for permuting the 28 bits stored in the third and the fourth registers, thereby generating the second subkey.

8. (New) The apparatus as recited in claim 1, wherein the positive integer N is 64.